Abstract

Described are a system and method for maintaining confidential records of an individual over a publicly accessible network. The system and method provide adequate confidentiality of the confidential records, mobility of individual access to the records, security of the data in the records, individual control of the confidential records, and integration with institutional information systems. The individual selects a publicly accessible record server for storing a confidential record. The confidential record is encrypted and stored by the gateway system on the selected record server. A predetermined agent is given an access token for accessing the confidential record over the network through the gateway server system. In a medical context, for example, the predetermined agent can be a health care institution, a medical research facility, or the individual who is a patient. The individual determines the privileges for the predetermined agent for accessing the confidential records. Such privileges can include reading, creating, modifying, annotating, and deleting. The individual also determines each portion of the confidential record that is accessible to the predetermined agent.

852035